

BITS

FINANCIAL SERVICES
R O U N D T A B L E

Filed via online portal

July 12, 2012

Federal Communications Commission
Office of the Secretary
Room TW-A325
445 12th Street SW
Washington, DC 20554

RE: CC Docket No. 96-115; DA 12-818
Privacy and Security of Information Stored on Mobile Communications Devices

To Whom It May Concern:

BITS¹, the technology policy division of The Financial Services Roundtable, appreciates the opportunity to provide comment to the Federal Communication Commission (FCC) on Privacy and Security of Information Stored on Mobile Communications Devices.

As the Commission has noted, technologies and business practices in the mobile marketplace are constantly evolving and rapidly changing. With each new function and product, new participants are introduced to this space. We believe it is essential for all participants to have appropriate security and privacy controls. We commend the FCC for their recognition of the important role that mobile wireless service providers have in the mobile marketplace.

As mobile devices gain capabilities similar to those of personal computers, it is essential that security and privacy standards be applied consistently. Many of our members offer consumers access to various services via mobile communications devices. Institutions offer services in three key areas: banking, payments and the mobilization of services such as remote deposit capture.

As with any financial transaction, security and privacy are critical. The mobile system is complex and interdependent, involving wireless service providers, device manufacturers, operating system developers, application developers and many new entrants seeing the promising opportunities of the

¹ BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs. For more information, go to <http://www.bits.org/>.

space. Given the complex and interdependent nature of the system, effective security and privacy solutions will require commitment and active involvement from all stakeholders.

We believe consumers must actively engage in their own security and privacy. Thus, our members educate consumers on methods to safely access their accounts through a variety of channels, including mobile. Mobile wireless service providers also interact with their customers regularly and should recognize this as an opportunity to educate on safe practices.

Mobile communications devices are designed to allow consumers to customize and control information on the device. Beyond financial information, consumers access many types of private data (e.g., contacts' information, emails). If a consumer recognizes that their device has been lost or stolen and notifies their the mobile wireless service provider, upon the authorized owner's request, the mobile wireless service provider should be required to remotely "freeze" or clear the data from the device and disable the subscriber identity module (SIM) card . This will greatly decrease the time frame for someone to access the information on the device for fraudulent or threatening behavior. This process would be very similar to the current process in place at financial institutions to cancel payment cards when they are reported lost or stolen.

Further, after being notified of a lost or stolen mobile device, the mobile wireless service provider should educate the consumer to promptly notify their financial institution if financial information was stored on the device. By providing consumers with a solution to a lost or stolen mobile device, we can empower consumers to be responsible for their security and privacy.

The disclosure of privacy policies are critical to consumers to ensure they are informed about the use and distribution of their information. Mobile communications devices present unique challenges in the distribution of privacy notices given their size and functionality constraints. We encourage the FCC to leverage and not duplicate industry efforts to develop codes of conduct for mobile privacy notifications, such as the multi-stakeholder process hosted by Department of Commerce's National Telecommunications and Information Administration.

Conclusion

In closing, we thank the FCC for addressing the issues of security and privacy on mobile communication devices. We encourage the FCC to recognize the critical role of mobile wireless service providers in the privacy and security of consumers.

If you have any questions or comments, please feel free to contact me at 202-589-2437 or PaulS@fsround.org, or Nicole Muryn, BITS Director of Regulation and Legislation, at 202-589-2435 or Nicole@fsround.org.

Sincerely,

A handwritten signature in dark ink, appearing to read "Paul N. Smocer". The signature is fluid and cursive, with the first name "Paul" and last name "Smocer" clearly legible.

Paul Smocer
President